TRS Policy — Prohibited Technologies

PURPOSE

The purpose of this policy is to limit security risks to TRS associated with the use of prohibited hardware and software products. On December 7, 2022, Governor Greg Abbott required (https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf) all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan providing state agencies guidance on managing personal devices used to conduct state business.

In addition to TikTok, Teacher Retirement System (TRS) may add other software and hardware products with security concerns to this policy and will be required to remove prohibited technologies which are on the DIR prohibited technology list.

CORE VALUES: This policy ties to TRS' commitment to its core values including accountability.

REFERENCE:

- Governor's Directive dated December 7, 2022
- Texas Government Code Chapter 620, Use of Certain Social Media Applications and Services on Governmental Entity Devices Prohibited.
- Governor's Proclamation dated January 31, 2025, regarding Ban on Chinese AI and Social Media Apps.

APPLIES TO: All TRS employees and non-TRS workers.

Note: Non-TRS workers assigned to TRS are expected to adhere to the standards of conduct outlined in this policy while on TRS premises or otherwise conducting TRS business.

DEFINITIONS:

"Prohibited Technologies" means:

(A) the social media service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited;

(B) a social media application or service specified by proclamation of the governor under Texas Government Code Section 620.005; or

(C) the software, applications, developers, hardware, equipment, and manufacturers listed on Addendum B.

"Sensitive location" means any location, physical, or logical (such as video conferencing, or electronic meeting rooms) identified as sensitive by TRS because it is used to discuss confidential or sensitive information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

"Unauthorized devices" means those that are manufactured by or contain one or more of the applications that are listed on the DIR Prohibited Technologies website at https://dir.texas.gov/information-security/prohibited-technologies.

POLICY STATEMENT

STATE-OWNED DEVICES

Except where approved exceptions apply, the use or download of Prohibited Technologies is prohibited on all TRS-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

TRS must identify, track, and control TRS-owned devices to prohibit the installation of or access to all Prohibited Technologies. This includes the various Prohibited Technologies for mobile, desktop, or other internet capable devices. These Prohibited Technologies may change over time.

TRS will manage all TRS-owned and issued mobile devices by implementing the security controls listed below:

a. Require installation of applications only from TRS-approved sources (see Addendum A).
b. Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
c. Maintain the ability to remotely uninstall unauthorized software from mobile devices.
d. Deploy secure baseline configurations, for mobile devices, as determined by TRS.

PERSONAL DEVICES USED FOR STATE BUSINESS

TRS and state business will not be conducted on TRS employee personal devices except in compliance with this policy. TRS and state business includes accessing any TRS data, applications, email accounts, non-public facing communications, state email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other state databases or applications. Loading an authenticator application alone to a personal device, without accessing any TRS or state information resources,

does not constitute conducting TRS or state business that would require removal of prohibited applications from that personal device.

TRS will issue devices to employees based on business need. If an employee or contractor has a justifiable TRS business requirement for the use of personal devices to conduct TRS business, they may request to use their personal device and, if approved, agree in writing to protect TRS applications and data in compliance with the TRS Mobile Device Policy. Using a personal device to conduct personal or state business means that the employee must remove and not install prohibited applications on this personal device.

Use of a personal device for TRS or state business requires compliance with this policy, the TRS Mobile Device Policy, the TRS Acceptable Use Policy, TRS Information Security Policies and Standards, TRS Confidentiality Policy and other applicable TRS policies.

2.3. Identification of Sensitive Locations

Sensitive locations must be identified, cataloged, and labeled by TRS. TRS will post appropriate signage regarding sensitive locations.

All reasonable precautions should be taken by employees, non-TRS workers, and visitors to ensure that Unauthorized devices such as personal cell phones, tablets, or laptops do not enter identified Sensitive locations, which includes any electronic meeting labeled as a Sensitive location, unless a justifiable need is documented, and an exception is granted by the Executive Director.

2.4. Network Restrictions

DIR has blocked access to Prohibited Technologies on the Texas state network. To ensure multiple layers of protection, to the extent possible, TRS will also implement additional network-based restrictions to include:

a. Configuring TRS technology and systems to block access to statewide Prohibited Technologies.
b. Prohibiting personal devices with Prohibited Technologies installed from connecting to TRS technology infrastructure or state data.
c. Providing a separate network for access to Prohibited Technologies with the approval of the Executive Director.
d. Providing a separate guest network that otherwise complies with this policy.

ONGOING AND EMERGING TECHNOLOGY THREATS

To provide protection against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this policy.

DIR will host a site that lists all Prohibited Technologies including apps, software, hardware, or technology providers. The Prohibited Technologies list current as of January 31, 2025, can be found at Addendum B. New technologies will be added to the list after consultation between DIR and DPS.

TRS will review the DIR Prohibited Technologies list regularly and will implement the prohibition and removal of any listed technology. TRS may prohibit technology threats in addition to those identified by DIR and DPS.

EXCEPTIONS

Exceptions to the ban on Prohibited Technologies may only be approved by the Executive Director. This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide Prohibited Technologies must be reported to DIR.

Exceptions to the policy will only be considered when the use of Prohibited Technologies is required for a specific business need, such as enabling investigations or for sharing of information to the public during an emergency. For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period. To the extent practicable, exception-based use should only be performed on devices that are not used for other state business and on non-state networks.

VIOLATIONS

Violation of this policy by a TRS employee may be grounds for corrective action, including termination of employment without warning. (See Corrective Actions and Dispute Resolution Policy). Criminal acts may also be prosecuted under applicable federal and state laws, including Texas Computer Crimes Law (Texas Penal Code Title 7, §33.01-33.04).

Violation of this policy by a user who is not a TRS employee may result in the termination of the employment or contractual relationship with the offender. Criminal acts may also be prosecuted under applicable federal and state laws, including Texas Computer Crimes Law (Texas Penal Code Title 7, §33.01-33.04).

CROSS REFERENCE/RELATED DOCUMENTS

- Acceptable Use Policy
- Confidentiality Policy
- Mobile Device Policy
- Information Security Policies and Standards
- Corrective Actions Policy
- Non-TRS Workers Policy

Policy Type: Enterprise	First Issued: February 2023
Contact: Frank Williams; Kristi Glasgall	Last Review: February 2023
Department Sponsor(s): Information Security; Legal & Compliance	Next Review Due Date: April 2027
Reviewing Department(s): Information Security; Legal and Compliance	Version Number: V. 4.0 February 2025
Review Cycle: 3 years	Version Approved Date: 2/11/2025
Intranet Location: L&C SharePoint Policies & Procedures Page	Signed: DocuSigned by: Caasi Lamb 5E9E8D6ECA374E5...

This policy does not constitute a contract, a promise or guarantee of employment, or a guarantee of access to TRS premises or information resources, as applicable, and may be modified, superseded, or eliminated by TRS without notice to the employee.

ADDENDUM A

Approved Sources for Applications/App Stores

- Apple App Store
- Google Play Store

ADDENDUM B

The up-to-date list of Prohibited Technologies is published at https://dir.texas.gov/information-security/prohibited-technologies. The following list is current as of January 31, 2025.

Prohibited Software/Applications/Developers

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet
- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office
- DeepSeek
- Lemon8
- Moomoo
- RedNote
- TigerBrokers
- WeBull
- Any subsidiary or affiliate of the entities listed above.

Prohibited Hardware/Equipment/Manufacturers

- Huawei Technologies Company
- ZTE Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company
- SZ DJI Technology Company
- Hytera Communications Corporation
- Any subsidiary or affiliate of the entities listed above.